CLAIM AMENDMENTS

Claims 1-9 (canceled).

Claim 10 (withdrawn): An anti-alteration system for homepage, comprising:

a public-web-server computer retaining the safe-web-files encrypted from a usual web-content which includes non-executable files and at a user browser side computer executable file;

a CGI Gateway module for sending a request information to a CGI Gateway means, wherein when said public-web-server computer gets said request information from a user browser to executes a CGI (Common Gateway Interface) program, said request information is a URL format including IP address, comment and parameters, however said public-web-server does not execute said CGI program before doing generation process, send said request information to said CGI Gateway module only; and

a send request information to original-web-server means, in which at said CGI Gateway module, said request information is modified automatically to a new request that is received by said original-web-server and sent to said original-web-server which comprises;

means for using said modified request information got from said CGI Gateway module, executing CGI program in said original-web-server computer,

means for sending a http header and CGI output contents from said CGI program to said CGI Gateway at said public-web-server computer; and

means for sending a CGI output from said CGI Gateway module to a user's browser passing through a public-web-server or directly.

Claim 11 (withdrawn): An anti-alteration system for homepage, as recited in claim 10, wherein chaos encryption technology is used to do encryption/decryption.

Claim 12 (withdrawn): An anti-alteration system for homepage, as recited in claim 10, wherein said real_tim_check technique uses a message authentication technology using chaos theory.

Claim 13 (new): An anti-alteration system for web-content, comprising:

a public-web-server computer retaining safe-web-files encrypted from usual original web-contents including one or more kinds of static file and one or more kinds of dynamic file, and providing HTTP web server functions.

a private-web-server computer which retains said original usual web-content and connects said public-web-server computer though means for avoiding illegal access as well as through a firewall,

means for authentication checking, decrypting and sending a safe-web-file, wherein when a web visitor's request is received, said public-web-server computer checks said safe-web-file that if said safe-web-file is no illegally altered, deleted or replaced, said public-web-server computer sends back said web-content decrypted from said safe-web-file to said web visitor with http or other protocol; and

a recoverable means for encrypting said web-content to create said safe-web-file on said private-web-server computer, wherein when said safe-web-file is illegally altered as checked by real_time_check technique on said public-web-server, said altered safe-web-file is automatically restored from said private-web-server.

Claim 14 (new): The anti-alteration system, as recited in claim 13, wherein said recoverable means incorporates with chaos encryption technology to do encryption and decryption of said web-content for increasing the web server response speed and increasing security strong of whole system.

Claim 15 (new): The anti-alteration system, as recited in claim 13, further comprising a real_time_check module used on said public-web-server computer for linking to a decryption module of said authentication check means to said web server, wherein said decryption module is able to be controlled by events of request received from said web visitor though http protocol.

Claim 16 (new): The anti-alteration system as recited in claim 15, further comprising a real-time-check device which is able to use a symmetric-key encryption to decrypt said safe-web-contents when said web visitor's request is received.

Claim 17 (new): The anti-alteration system, as recited in claim 16, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

Claim 18 (new): An anti-alteration system for web-content, comprising:

a public-web-server computer, employed with a prohibit web-content illegally alter function, retaining safe-web-contents that have been added with a prohibit illegally alter header information including a MAC (Massage Authentication Code) generated by said original web-content, and properties of original-web-content including name, size, date, and location thereof;

a private-web-server computer which retains said original web-content and connects said public-web-server computer which is added with said prohibit illegally alter function, though a means of avoiding illegal access as well as through a firewall;

a real_time_check technique, in which when a web visitor's request is received, separates a header information is separated from a requested safe-web-file which is added with an avoiding illegally alter header, and at same time using said MAC(Message Authentication Code) included in said header information to check said safe-web-file by method of a message authentication technology;

separate header information, wherein said web visitor's request is received, said real-time-check technique is used to check said safe-web-file and when said safe-web-file is checked being not altered, said header information from said safe-web-file is cut and the rest part is changed to said web-content which is sent back from said public-web-server to said web visitor; and

a recoverable means for adding said header information to said original web-content to create a new safe-web-file on said private-web-server computer when an illegally altering of said safe-web-file is detected, wherein said new safe-web-file is sent

to said public-web-server computer to automatically restore said safe-web-file which is illegally altered.

Claim 19 (new): The anti-alteration system, as recited in claim 18, further comprising a real_time_check module used on said public-web-server computer for linking to authentication module to said web server, wherein said authentication module is able to be controlled by events of request received from said web visitor though http protocol.

Claim 20 (new): The anti-alteration system, as recited in claim 19, wherein said real_time_check module uses a message authentication technology using chaos theory to check whether the safe-web-content be altered or not.

Claim 21 (new): The anti-alteration system, as recited in claim 18, wherein said real_time_check module that is able to link said Web server to any other message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA to find said web-content altered when said web visitor's request is received.

Claim 22 (new): An anti-alteration system for web-content, comprising:

a public-web-server computer, employed with a prohibit web-content illegally alter function, retaining safe-web-files which have been encrypted from original web-contents and have been added with a prohibit illegally alter header information, including a MAC (Massage Authentication Code) generated from authentication checking said original web-content and properties including name, size, date, and location on a hard disk thereof;

a private-web-server computer which retains said original web-content and connects said public-web-server computer which is added with prohibit illegally alter and decryption functions, though a means of avoiding illegally access as well as through a firewall;

a real-time-check technique, wherein when a web visitor's request is received to obtain a requested safe-web file, a header information is separated from said safe-web-file which is added with an avoiding illegally alter header, and at the same time using a

MAC (Message Authentication Code) included in said header information to check said safe-web-file by method of a message authentication technology;

separate header information, wherein when said web visitor's request is received, said real-time-check technique is used to check said safe-web-file and when said safe-web-file is checked being not illegally altered, said header information is cut from said safe-web-file and the rest part is decrypted to said web-content which is sent back from said public-web-server computer to said web visitor; and

a recoverable means when an illegally altering of said safe-web-file is detected, encrypting said original web-content and adding a header information to said original web-content to create a new safe-web-file on said private-web-server computer, sending said new safe-web-file to said public-web-server computer to automatically restore said safe-web-file which has been altered.

Claim 23 (new): The anti-alteration system, as recited in claim 22, wherein said recoverable means incorporates with chaos encryption technology to do encryption and decryption of said web-content for increasing the web server response speed and increasing security strong of whole system.

Claim 24 (new): The anti-alteration system, as recited in claim 22, further comprising a real_time_check module used on said public-web-server computer for linking to decryption module and authentication module to web server, wherein said decryption module and authentication module is adapted to be controlled by events of request received from said web visitor though http protocol.

Claim 25 (new): The anti-alteration system, as recited in claim 23, wherein said real-time-check device is able to use a symmetric-key encryption to decrypt said safe-web-contents when said web visitor's request is received.

Claim 26 (new): The anti-alteration system, recited in claim 25, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

Claim 27 (new): The anti-alteration system, as recited in claim 24, wherein said real_time_check module uses a message authentication technology using chaos theory to check whether the safe-web-content be altered or not.

Claim 28 (new): The anti-alteration system, as recited in claim 24, wherein said real_time_check module that is able to link said web server to any other message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA to find said web-content altered when said web visitor's request is received.